Outlook

Re: Ransomeware Recovery Plan

From Maria Fontana <originalines@hotmail.com>
Date Tue 2/18/2025 10:16 PM
To Karimi . Najera Garcia <knajera@lamar.edu>; Nilka Quinones <nilkaquinones2@gmail.com>; Tytiauna Goode <tgoode1@lamar.edu>; katia soto <katiaysoto@gmail.com>

Dear Team Leaders,

I'd like to commend you all on your exceptional leadership in strategically, effectively, and collaboratively managing this cyberattack. I encourage our team to compile a final report detailing each event of the crisis. This will serve as a foundational element in our incident response strategy and as a critical tool in enhancing our organization's security posture.

As a servant leader, my focus is on crafting incident reports that serve as actionable blueprints for remediation and growth. Every detail—from documenting the immediate response to conducting a thorough root cause analysis—contributes to building a more resilient and proactive security framework. Let's design this report with care and intention to understand, efficiently resolve security breaches, and provide valuable insights for preventing future incidents.

To finalize the investigation, strategies, and action plan to address the cybersecurity attack, creating a comprehensive report is essential. This report helps us move forward while acknowledging the importance of all affected individuals.

Again, I'm deeply impressed by the hard work and dedication of all the team leaders. Therefore, ensure our incident report integrates your needs and final concerns, your insights and suggestions are invaluable. By incorporating your feedback, we ensure the report captures technical details and reflects the practical experiences and challenges faced by those on the front lines. This empowers you to handle similar situations effectively in the future. The ultimate purpose of an incident report goes beyond merely recording what went wrong. It is about identifying opportunities for improvement and fostering a culture of continuous learning. Whether it involves upgrading technology, revising security policies, or educating our team members, the lessons learned from detailed incident reporting empower us to stay ahead of evolving threats.

In the end, consistent, accurate, and insightful incident reporting transforms challenges into opportunities for growth. It ensures our organization is better prepared to face the ever-changing cybersecurity landscape, with a focus on serving and protecting our stakeholders.

Sincerely,

Maria Ines Fernandez

Team Leader.

From: Karimi . Najera Garcia <knajera@lamar.edu>
Sent: Tuesday, February 18, 2025 1:15 PM
To: Nilka Quinones <nilkaquinones2@gmail.com>; Tytiauna Goode <tgoode1@lamar.edu>; Maria Fontana <originalines@hotmail.com>; katia soto <katiaysoto@gmail.com>
Subject: Re: Ransomeware Recovery Plan

I would like to take a moment to express my gratitude to everyone for your collaboration on this issue. As I have mentioned previously, each of us plays an important role in finding a solution. One aspect that stood out to me was the consistent communication among all of us leaders, which reflects our commitment to working together.

While we may have differing ideas, our ultimate goal remains the same. I believe that by continuing to collaborate, we can prevent similar issues in the future.

Tytianna, I appreciate the thoroughness of your plan, particularly the timeline, which is critical for our success.

Maria, thank you for your ongoing concern for our community; it is essential for us to keep this in mind as we work to rebuild trust.

Katia, your approach to Continuous Review and Adjustment of the Plan is vital for all of us to consider in our efforts to mitigate future cyber threats.

Nilka, your organized timeline for gathering input from key departments is key to ensuring effective communication.

Once again, thank you all for sharing your ideas. I believe we have all gained valuable insights that will aid us in developing more effective plans for our campuses.

Team Leader,
Karimi Najera Garcia

From: Nilka Quinones <nilkaquinones2@gmail.com>
Sent: Sunday, February 16, 2025 6:54 PM
To: Tytiauna Goode <tgoode1@lamar.edu>; Maria Fontana <originalines@hotmail.com>; katia soto <katiaysoto@gmail.com>
Cc: Karimi . Najera Garcia <knajera@lamar.edu>
Subject: Re: Ransomeware Recovery Plan

Dear Team Leaders,

I want to take a moment to recognize and commend the outstanding collaboration, strategic thinking, and dedication that have brought us to this point. The way we have aligned our expertise to address the ransomware attack speaks volumes about our collective commitment to organizational resilience.

After reviewing our agreed-upon plan, I fully support the structured approach we have outlined. Our focus on stakeholder communication, access to teaching materials, financial aid processing, and long-term cybersecurity measures ensures that we are addressing both the immediate impact and reinforcing our defenses against future threats. This plan not only restores operational stability but also positions us for stronger, more proactive cybersecurity management moving forward.

As we transition into execution, our ability to stay agile, anticipate challenges, and maintain cross-functional coordination will be key to a successful implementation. By following the proposed timeline and maintaining open lines of communication, we will ensure that each phase is executed with precision and accountability.

With this resolution, we bring closure to this cybersecurity incident and pivot towards fortifying our infrastructure, refining our policies, and institutionalizing a culture of cybersecurity awareness. This moment serves as both a lesson and an opportunity, one that strengthens our resilience and reaffirms our commitment to safeguarding our institution.

I extend my deepest appreciation to each of you for your leadership, diligence, and unwavering support. Your contributions have been instrumental in turning this challenge into a catalyst for long-term improvement. I look forward to continuing this momentum as we implement and reinforce our security measures.

Let’s move forward with confidence and clarity.

Best regards,
Nilka V. Quinones Rodriguez

Team Leader

From: Tytiauna Goode <tgoode1@lamar.edu>
Date: Sunday, February 16, 2025 at 2:16 PM
To: Maria Fontana <originalines@hotmail.com>, katia soto <katiaysoto@gmail.com>
Cc: Nilka Quinones <nilkaquinones2@gmail.com>, Karimi . Najera Garcia <knajera@lamar.edu>
Subject: Re: Ransomeware Recovery Plan

Hello Team,

I am overjoyed with our ability to come together and collaborate on the best course of action to address the ransomware attack. After reviewing all of our ideas, it seems that we have agreed upon the following plan:

Stakeholder Communication:
Once we finalize this plan, we will begin communicating with stakeholders to ease concerns and inform them of the next steps. We will evaluate our current communication touchpoints to identify what has been effective and where enhancements are needed. Additionally, we will work with the IT department to develop a feedback forum to better understand student and staff needs and direct our efforts accordingly. Phased updates will be sent to ensure that information is shared strategically, with clarity and precision.

Access to Teaching Materials:
We will consult with leaders in the Teaching & Learning department to ensure they have a level of decision-making agency in this process. We will also communicate with the board to align expectations with the required rigor of our courses.

Financial Aid Processing:
We will work with the board to assess the level of flexibility we have in extending processing

deadlines. If necessary, we will seek an external partner to assist the Financial Aid department in processing aid quickly.

Preventing Future Occurrences:

- Implement multi-factor authentication to enhance secure access.
- Incorporate periodic cybersecurity training for faculty.
- Consult with the board about the possibility of purchasing an external IT protection service.
- Establish a dedicated cybersecurity committee to regularly evaluate policies, recommend improvements, and stay ahead of emerging threats.
- Secure ongoing budget allocations for cybersecurity infrastructure and staff training.

Implementation Timeline:

- **Phase 1 (Next 3–5 Days):** Initial outreach to IT, Financial Aid, and Teaching & Learning to outline key concerns and gather preliminary insights.
- **Phase 2 (Week 2):** Synthesis of department feedback into a working draft, ensuring feasibility, alignment with operational constraints, and organizational fit.
- **Phase 3 (Week 3):** Cross-departmental review and finalization of an integrated response plan before external communication begins.

I have done my best to compile everyone's feedback into a straightforward and simplified plan that will help us get started more easily. Please review and let me know if anything needs adjustment so we can begin implementation ASAP.

Best,
Tytiauna Goode
Team Leader

From: Maria Fontana <originalines@hotmail.com>
Sent: Sunday, February 16, 2025 10:33 AM
To: katia soto <katiaysoto@gmail.com>
Cc: Nilka Quinones <nilkaquinones2@gmail.com>; Tytiauna Goode <tgoode1@lamar.edu>; Karimi . Najera Garcia <knajera@lamar.edu>
Subject: Re: Ransomeware Recovery Plan

Dear Team Leaders,

I deeply appreciate the meticulous strategies that have been outlined to mitigate this cybersecurity crisis. While these plans are critical, I believe that our most important goal is to address the needs of our people.

The students, teachers, and staff are grappling with concerns, feelings of frustration, and various impediments due to this cyber-attack. Their voices need to be heard through active listening, and we must prioritize their well-being and restore their autonomy.

To support this, I propose that:

1. We actively listen to all those affected, ensuring their concerns and feelings are acknowledged. After addressing their needs, we should also reinstate trust among all members involved by entitling them to a free annual credit report from each of the three major credit reporting agencies.

2. Teachers should be empowered to create their own grading system to maintain continuity in education until the crisis is resolved.

3. Our financial staff team should receive support from external accounting resources to expedite and manage any financial transactions for the 15,000 students impacted.

Our primary focus should be on the well-being and empowerment of our community, ensuring that they feel supported and heard throughout this challenging time.

Best regards,

Maria Ines Fernandez

Team Leader.

From: katia soto <katiaysoto@gmail.com>
Sent: Sunday, February 16, 2025 3:35 PM
To: Maria Fontana <originalines@hotmail.com>
Cc: Nilka Quinones <nilkaquinones2@gmail.com>; Tytiauna Goode <tgoode1@lamar.edu>; Karimi . Najera Garcia <knajera@lamar.edu>
Subject: Re: Ransomeware Recovery Plan

Dear Team Leaders,

Our approach to this crisis must be strategic, flexible, and focused on institutional resilience. This situation has demonstrated that there is no single solution; instead, we must adopt an adaptable framework that enables us to respond immediately while simultaneously building a more secure infrastructure for the future. Below, I propose a structured solution that will allow both the mitigation of the current problem and the prevention of future incidents.

1. **Internal Assessment Phase and Immediate Response**
   Before making any external communication, we must assess our internal capacity and verify that our containment measures are functioning. To achieve this:
   - We will monitor real-time security to identify suspicious activity and prevent new vulnerabilities.
   - We will validate the effectiveness of containment measures implemented by the IT team and ensure that our systems are not accessed unauthorized.
   - We will coordinate with each key department (IT, Finance, Teaching & Learning, and Administration) to ensure that internal teams are aligned and prepared before external communication.
   - We will conduct a controlled data recovery test, ensuring our backup copies are functional and secure.

2. **Implementation of an Adaptive Communication Plan**
   - Poorly managed communication can generate panic and distrust. To avoid this, I propose:
   - Differentiated communication strategies based on the audience (students, faculty, administrative staff, and external stakeholders), ensuring each group receives relevant information.
   - Phased update messages allow information to be shared strategically, ensuring clarity and precision.
   - Creation of a communication response team responsible for addressing concerns and providing accurate information, preventing the spread of misinformation.

3. **Strengthening Security and Operational Continuity**
   To ensure the recovery and continuity of our operations, I propose the following:
   - Enhancing secure access: Accelerated implementation of multi-factor authentication and restrictions on sensitive databases.

- Creating a secure environment for virtual learning: Temporary storage alternatives to prevent interruptions in access to educational materials.
- Optimizing the financial aid process: Ensuring students can access their benefits without unnecessary delays.

4. **Developing a Continuous Learning Strategy for Cybersecurity**

This crisis has highlighted the need to strengthen our organizational culture regarding cybersecurity. To achieve this:

- Periodic cybersecurity training for faculty, administrative staff, and students.
- Cyberattack simulations to assess the IT team's response and improve preparedness for future incidents.
- Create a cybersecurity committee responsible for monitoring trends and preventing threats before they escalate into crises.

5. **Continuous Review and Adjustment of the Plan**

Adaptive leadership requires evaluating and modifying our strategies as challenges evolve. To accomplish this:

- Periodic meetings will be established to assess the impact of implemented measures and make adjustments as needed.
- Success metrics will be integrated, allowing us to monitor the effectiveness of applied solutions.
- A continuous improvement framework will be developed, ensuring that the institution remains prepared for future cybersecurity threats.

Beyond resolving the current crisis, our approach must create a resilient and adaptable system that enables us to face future threats confidently and efficiently. The ability to respond quickly, learn from each situation, and strengthen our defenses will define our institution's success in the digital era.

I look forward to collaborating on executing this strategy and ensuring that our community not only overcomes this crisis but emerges stronger from it.

Sincerely,
Katia Y. Soto Hernandez
Team Leader

On Sat, Feb 15, 2025 at 8:04 PM Maria Fontana <originalines@hotmail.com> wrote:

> Dear Team Leaders,
>
> As a servant leader, I would like to take this opportunity to express my gratitude to my colleagues, Karimi Najera Garcia, Tytiauna Goode, Nilka Quinones, and Katia Soto for the time they took to respond to the cyber attack.
>
> Karimi, I completely agree with you on the way to create awareness on cybersecurity, limit access to data, and ensure proper communication. These are crucial in protecting our institution from various threats. Tytiauna, I completely agree with you on the need to ensure that information is received and given to the right people at the right time, and this is something that I support wholeheartedly.
>
> The suggestion of an interactive webpage for stakeholders and the formation of a diverse crisis response team are great ways of ensuring that the entire community is informed and included in

decision making. Nilka, your approach of breaking down the issues into steps of communication, guaranteeing the continuity of teaching and learning, and increasing data security is a correct identification of the different aspects of the problem. Your thoughts are precious to me.

Katia, I appreciate your concern to involve internal services before contacting external ones. Your suggestion of a flexible and adaptive approach is very important in managing the risks and challenges that come with a crisis. So, as we move forward, it is important that we as leaders adopt the servant leadership approach and focus on the needs of the stakeholders and their welfare.

Indeed, communication, stakeholder relationships and coordination between different departments are critical. For the remaining issues, the following recommendations are made:

• **Finalize the Communication Strategy:** We should set up a working group to design a specific communication strategy that would involve working with internal and external stakeholders. This plan should define the roles and responsibilities of each department during the crisis.

• **Establishing crisis Response Teams:** It would be advisable to set up crisis response teams that will include the IT, Financial Aid, Teaching & Learning and other important departments. These teams should be trained and practiced responding appropriately during crisis situations.

• **Consulting Key Departments:** When we work with IT, Financial Aid, Teaching & Learning and other relevant departments, we will be able to understand their needs and challenges. It is through this collaborative approach that we will be able to come up with solutions that will improve our cybersecurity posture as a district.

• **External IT Protection:** I recommend the use of external IT protection services such as ClassLink. Through our CTO, we can get the best guidance and resources that will help us improve our security. It is crucial to make sure that any of the protection measures to be implemented do not violate the Children’s Online Privacy Protection Act (COPPA).

Concerning security, ClassLink protects the data transmitted to vendor companies, and it can redact information using the new DataGuard. The multifactor authentication (MFA) gives an additional level of security. Furthermore, ClassLink is a member of the Cybersecurity Coalition for Education and has come up with the Cybersecurity Group Break.

This proactive approach can really benefit our district by keeping us informed on all aspects of security, strengths and weaknesses and areas of improvement. The group offers free membership, updates, and the possibility to work together. The rubric evaluators from other districts will help us to reassess our security and develop a proactive strategy.

ClassLink has protected the information of over 21 million users across more than 2,800 school districts and has proven its ability in protecting the information. Last, building a strong network relationship and making sure our CTO is part of this group will be important. To be system leaders, we all must become strategic thinkers and use resources like CoSN.org membership.

It is also important to note that it is not only the issue of communication but also the issue of the needs of society, their welfare and involvement. We need to comprehend and listen to assist, support and protect everyone involved in this crisis, including stakeholders.

Thus, suggesting the use of ClassLink, we are determined to prevent any further attacks and work towards the solutions rather than the problems. This approach enables the restoration of respect, participation, and productivity in the long run, based on empathy.

I would like to address everyone at a mutual consensus and in line with the college’s values and principles to decide and learn from our mistakes. These measures will assist in establishing a strong and supportive community while at the same time reducing the risks posed by cyber-attacks. I look forward to working with you all to put these plans into action and achieve our goal of protecting our institution.

Regards,
Maria Ines Fernandez
Team Leader,

From: katia soto <katiaysoto@gmail.com>
Sent: Saturday, February 15, 2025 3:53 AM
To: Nilka Quinones <nilkaquinones2@gmail.com>
Cc: Tytiauna Goode <tgoode1@lamar.edu>; Karimi . Najera Garcia <knajera@lamar.edu>; originalines@hotmail.com <originalines@hotmail.com>
Subject: Re: Ransomeware Recovery Plan

Dear Team Leaders,

Ensuring clear communication channels and effective internal coordination is critical to successfully managing this crisis. The proposed timeline provides a solid foundation, maintaining momentum while allowing for adjustments when necessary. We should integrate an adaptive review process into each phase. While structured planning is essential, real-time developments may require us to re-evaluate priorities or adjust our approach as new information emerges. To ensure our response remains agile, we should:

- **Build flexibility into the communication plan:** As we evaluate existing channels, we should ensure room for iterative adjustments based on stakeholder feedback and emerging needs. An overly rigid approach might not capture all concerns as they evolve.
- **Continually assess internal constraints:** While the proposed timeline ensures a diligent process, we should be open to modifying timelines or priorities based on operational challenges that may arise. Periodic reviews at key moments will help us dynamically refine our strategy.
- **Strengthening our rapid response capabilities:** While structured implementation is important, we must also ensure that we can act quickly in the face of unforeseen developments. A designated team that can pivot agilely in emergencies will strengthen our ability to manage uncertainty effectively.

By maintaining a structured yet adaptable approach, we can balance internal alignment with the reality of an ever-evolving crisis. During each phase, we must remain vigilant about changes in the situation and adjust our strategies based on new needs and challenges that may arise.

> I will continue to collaborate to define and implement a response strategy that is both effective and flexible.
>
> Sincerely,
>
> Katia Soto Hernadez
> Team Leader
>
> On Fri, Feb 14, 2025 at 9:08 PM Nilka Quinones <nilkaquinones2@gmail.com> wrote:
>
> > Dear Team,
> >
> > I appreciate the collective insight and commitment each of you brings to this process. We are clearly aligned in our priorities, transparency, stakeholder engagement, and cross-departmental collaboration, which will be instrumental in executing a well-structured and operationally effective response.
> >
> > To establish the most effective communication channels for our stakeholders, I recommend we begin by assessing existing communication frameworks (e.g., open office hours, town halls, and feedback mechanisms) and identifying any gaps or opportunities for improvement. A targeted approach will allow us to introduce structured, high-impact engagement strategies rather than implementing fragmented efforts. To determine the best course of action, I propose that we:
> >
> > 1. Evaluate current communication touchpoints to identify what has been effective and where we need enhancement.
> > 2. Designate a working group to outline a structured communication plan that aligns with our institutional priorities.
> > 3. Pilot and refine communication strategies before full-scale implementation, ensuring consistency and clarity in messaging.
> >
> > By structuring our stakeholder engagement efforts this way, we will ensure that all messaging is cohesive, purposeful, and strategically timed to reinforce confidence rather than create uncertainty.
> >
> > To maintain momentum while ensuring due diligence, I recommend setting a structured timeline for gathering input from key departments. A practical approach would be:
> >
> > - Phase 1 (Next 3–5 Days): Initial outreach to IT, Financial Aid, and Teaching & Learning to outline key concerns and gather preliminary insights.
> > - Phase 2 (Week 2): Synthesis of department feedback into a working draft, ensuring feasibility, alignment with operational constraints, and organizational fit.
> > - Phase 3 (Week 3): Cross-departmental review and finalization of an integrated response plan before external messaging begins.
> >
> > This structured timeline allows for thorough internal coordination while maintaining the urgency for an effective response. If this timeline aligns with our shared expectations, we can implement it accordingly.
> >
> > We have the right foundational elements to navigate this challenge effectively as a team. We will mitigate immediate concerns and reinforce institutional resilience and stakeholder trust in the long

term by ensuring internal alignment, maintaining operational agility, and communicating with precision. I look forward to working alongside you to refine and execute a measured and impactful approach.

Best,
Nilka V. Quinones Rodriguez
Team Leader

From: Tytiauna Goode <tgoode1@lamar.edu>
Date: Friday, February 14, 2025 at 2:33 PM
To: katia soto <katiaysoto@gmail.com>, Nilka Quinones <nilkaquinones2@gmail.com>
Cc: Karimi . Najera Garcia <knajera@lamar.edu>, originalines@hotmail.com <originalines@hotmail.com>
Subject: Re: Ransomeware Recovery Plan

Team Leaders,

First, I want to thank everyone for your thoughtful contributions. It's clear from our discussions that we all share a strong commitment to transparency, stakeholder engagement, and collaboration. These values will be central to our success as we navigate this situation together.

We all recognize the importance of ***clear and transparent communication***. Our stakeholders (students, faculty, and families) rely on us to keep them informed, and we're united in our belief that proactive communication will help maintain trust, reduce uncertainty, and avoid speculation. Whether it's through **open office hours**, **town hall meetings**, or **continuous feedback mechanisms**, we all agree that staying connected with our community is essential. I am hoping that we can work together to determine the best course of action to create and introduce these channels.

Additionally, the importance of ***collaborating across departments*** is another point of alignment. We understand that no decision or plan should be finalized without consulting those who will be impacted, especially in areas like finance and technology. By ensuring that our internal teams, IT, Financial Aid, Teaching & Learning, and Administration, are fully aligned and prepared, we set ourselves up for a seamless implementation process. What sort of timeline should we set to gauge feedback from these departments and move forward with a plan?

That said, while these commonalities are crucial for our progress, there are a few areas where we can refine our approach to ensure we're as effective as possible.

First, I think we need to be mindful of **timing**. As we move forward, we must balance the urgency of communication with the need to ensure our internal teams are fully aligned. I understand that my premature communication, while well-intentioned, can often lead to confusion and additional challenges that we're not yet prepared to handle. We've all acknowledged the need to communicate frequently and transparently, but after hearing your input, I believe we must stabilize our internal operations first, assessing the scope of the issue and making sure our teams are aligned. This will allow us to present a unified, clear, and well-supported message to our community. Thank you for your input on this. It's important to me that we carefully balance urgency with internal alignment, and I appreciate your perspective in helping me see how we can strengthen our approach.

Secondly, I am committed to engaging with key departments, but after internalizing your feedback, I understand we should ***strengthen our internal coordination*** before doing so. Before we move forward with finalizing any plans, it's critical that we have comprehensive buy-in from all involved parties, especially in areas that have direct impacts on our resources and infrastructure. This internal alignment is necessary to ensure that when we communicate externally, we're delivering a message that is consistent, accurate, and well-informed. With your support, I will wait to reach out to other departments until we have reached a consensus on our plan.

Lastly, I encourage us to **stay flexible** in our approach. The landscape is rapidly evolving, and while we've laid out a plan for communication, we must be ready to adjust our strategy based on real-time developments and feedback. We still need to develop a concrete plan to address financial aid complications, access to teaching materials, and data security.

As a team, we have all the right elements in place to succeed: transparency, stakeholder engagement, and cross-departmental collaboration. Let's work together to refine our approach by ensuring that we take the necessary time to align internally, stay adaptable, and communicate with precision and clarity.

I'm confident that by combining our strengths, we will create a response that is not only effective in the short term but also strengthens trust and stability for the long-term future of our institution.

Thank you, and I look forward to working alongside each of you as we move forward with this important work.

From: katia soto <katiaysoto@gmail.com>
Sent: Thursday, February 13, 2025 10:00 PM
To: Nilka Quinones <nilkaquinones2@gmail.com>
Cc: Tytiauna Goode <tgoode1@lamar.edu>; Karimi . Najera Garcia <knajera@lamar.edu>; originalines@hotmail.com <originalines@hotmail.com>
Subject: Re: Ransomeware Recovery Plan

Dear Team Leaders,

I am grateful for the valuable insights and collaborative effort each of you has contributed to addressing this cybersecurity crisis. The diverse perspectives shared highlight the strength of our team in tackling this challenge effectively. Transparency and communication are essential, but we must ensure that our first step is not rushed but strategically informed. While I understand the intent behind quickly addressing external stakeholders, premature communication without a fully developed internal response can lead to misinformation, increased uncertainty, and additional challenges that we may not yet be prepared to handle.

> > Before engaging external stakeholders, we must focus on stabilizing our internal operations and ensuring that each IT, Financial Aid, Teaching & Learning, and Administration department has the information, tools, and coordinated approach to respond effectively. Without this alignment, external communication may create more confusion than clarity.
> >
> > To achieve this, I propose:
> >
> > 1. Assessing the Internal Situation First,
> >   We must thoroughly evaluate the scope of the breach, define immediate priorities, and coordinate our internal teams before releasing external statements. Additionally, all internal teams must have the same information to avoid contradictory messages, which could create confusion among students, staff, and other key groups.
> >
> > 2. Validating Our Communication Before Sharing It Externally:
> > I propose establishing an internal validation process where each key department reviews the information before sharing it externally. This would ensure accuracy and consistency in our messaging.
> >
> > 3. Implementing a Strategic and Flexible External Communication Plan:
> > Once our internal teams are aligned and prepared, we can initiate external communication strategically, clearly, and effectively. Our messaging should evolve based on real-time developments and internal progress, ensuring we remain flexible and responsive to changing circumstances.
> >
> > 4. Monitoring and Adjusting Our Communication Strategy:
> > To ensure effective communication, we should implement a feedback mechanism to evaluate how messages are received and adjust our strategy accordingly.
> >
> > A reactive approach to communication may provide short-term reassurance, but it can also create long-term confusion if not backed by a solid internal strategy. Our role is to ensure that every action we take is informed, strategic, and capable of evolving as new information emerges.
> >
> > Let's first align internally, build a strong foundation, and then communicate externally to reinforce trust, not uncertainty. I look forward to working with all of you to refine this approach.
> >
> > Best,
> > Katia Y. Soto Hernandez
> > Team Leader
> >
> > On Thu, Feb 13, 2025 at 9:07 PM Nilka Quinones <nilkaquinones2@gmail.com> wrote:
> >
> > > Dear Tytiauna
> > >
> > > I appreciate your commitment to transparency and stakeholder engagement. While I recognize early communication's challenges, I also acknowledge the value of proactive and clear messaging during uncertain times. Maintaining trust with students, faculty, and families is a priority, and the right balance between timely updates and structured planning is key. Moving forward, we can refine our communication strategy to ensure that all messaging aligns with our broader response plan while keeping stakeholders informed in a way that builds confidence rather than concern.
> > >
> > > I strongly support establishing open office hours for students and faculty to provide direct access to information and support. This would allow us to address concerns proactively, reduce

speculation, and reinforce a sense of stability. In addition, implementing a continuous feedback process, whether through town halls, digital feedback mechanisms, or faculty engagement sessions, will help ensure that our response remains aligned with the evolving needs of our campus community. Faculty involvement in this process will be invaluable in maintaining open lines of communication and reinforcing institutional trust.

We must engage key departments before finalizing our plan, particularly in areas impacting financial and technological infrastructure. A collaborative and well-informed approach will ensure that our strategy is operationally viable, resource-efficient, and aligned with institutional objectives. I am fully committed to contributing to a preliminary framework. Still, I believe proactively securing input from these departments will allow us to anticipate potential challenges, optimize resource allocation, and drive a seamless implementation process. By integrating cross-functional expertise, we can strengthen decision-making and position our response for long-term success.

Let’s refine our approach with clear coordination, stakeholder engagement, and a well-executed implementation plan. I look forward to working together to ensure our response remains effective, transparent, and aligned with our institution’s long-term trust and stability.

Best,
Nilka V. Quinones Rodriguez

Team Leader

From: Tytiauna Goode <tgoode1@lamar.edu>
Date: Thursday, February 13, 2025 at 8:20 PM
To: Nilka Quinones <nilkaquinones2@gmail.com>, Karimi . Najera Garcia <knajera@lamar.edu>, katia soto <katiaysoto@gmail.com>
Cc: originalines@hotmail.com <originalines@hotmail.com>
Subject: Re: Ransomeware Recovery Plan
Good Evening Team,

I want to apologize again for prematurely reaching out to families. I understand that it may have unintentionally complicated our efforts to address the issue swiftly by introducing added concern from students and parents. That said, I still believe in the importance of maintaining open and frequent communication with our stakeholders to avoid leaving them uncertain about where things stand.

In addition, I would like to emphasize the importance of proactively addressing concerns by establishing open office hours for students and faculty. This would allow them to share concerns directly and receive support during this challenging time. Finally, I believe we should implement a continuous feedback process, whether through town hall meetings or feedback forms, to ensure our response remains aligned with the evolving needs of the campus community. Faculty involvement will be critical in facilitating this process, and I hope we can work together to make it as effective as possible.

From my perspective, I feel it's crucial that we consult the relevant departments before finalizing a plan, especially when it comes to financial or technology-related aspects. I’m more than willing to help develop a preliminary outline, but I think it's important that we check with these departments to ensure that the plan is feasible before moving forward.

Best,
Tytiauna

From: Nilka Quinones <nilkaquinones2@gmail.com>
Sent: Thursday, February 13, 2025 7:59 PM
To: Tytiauna Goode <tgoode1@lamar.edu>; Karimi . Najera Garcia <knajera@lamar.edu>; katia soto <katiaysoto@gmail.com>
Cc: originalines@hotmail.com <originalines@hotmail.com>
Subject: Re: Ransomeware Recovery Plan

Dear Team Leaders,

I appreciate the collective effort and strategic thinking everyone is bringing to this situation. Our shared commitment to resolving the ransomware attack efficiently and effectively is critical.

While I fully support the urgency of involving key departments like Financial Aid, IT, and Teaching & Learning in our decision-making process, we should establish a more structured approach before reaching out to external stakeholders. Ensuring we present a unified, data-driven, and solution-oriented message will strengthen confidence in our ability to manage this crisis.

On the topic of communication, I recognize the need for transparency and agree that prolonged silence could raise concerns. However, we must weigh the benefits of early communication against the risk of creating uncertainty without a solidified plan. While the message sent to students and parents is reassuring, I believe we should refine our external communication strategy by:

1. **Aligning on key messaging** – Ensuring we clarify what we know, what steps we are taking, and what stakeholders can expect moving forward.
2. **Timing updates strategically** – Rather than issuing frequent, incremental updates, we should aim for impactful, confidence-building communications at key decision points.
3. **Addressing potential concerns proactively** – Anticipating questions from students, parents, and staff so we can provide well-prepared, transparent responses.

I strongly agree that we need to activate our crisis response teams immediately to precisely manage different aspects of this situation. By establishing clear objectives within each team, we can ensure a cohesive and well-executed response.

I welcome further discussion on this approach. Aligning on a well-structured and coordinated response will strengthen our internal decision-making and external communication. I look forward to hearing your perspectives.

Best regards,
Nilka V Quinones Rodriguez
Team Leader

From: Tytiauna Goode <tgoode1@lamar.edu>
Date: Thursday, February 13, 2025 at 10:25 AM
To: Karimi . Najera Garcia <knajera@lamar.edu>, katia soto <katiaysoto@gmail.com>, Nilka Quinones <nilkaquinones2@gmail.com>
Cc: originalines@hotmail.com <originalines@hotmail.com>
Subject: Re: Ransomeware Recovery Plan
Karimi,

I am sorry if the email I sent to families was not in the best interest of the team. I was anxious to send a statement out as quickly as possible. Moving forward, I will be sure to make sure any stakeholder communication is approved by the leadership team. I hope we can get a move on these action items soon!

I know that you are all about inspiring other to work together toward a shared vision, so I'm eager to see how we will move forward.

Tytiauna Goode
Team Leader

From: Karimi . Najera Garcia <knajera@lamar.edu>
Sent: Thursday, February 13, 2025 9:37 AM
To: Tytiauna Goode <tgoode1@lamar.edu>; katia soto <katiaysoto@gmail.com>; Nilka Quinones <nilkaquinones2@gmail.com>
Cc: originalines@hotmail.com <originalines@hotmail.com>
Subject: Re: Ransomeware Recovery Plan

Dear Tytianna,

I believe it is essential for us to begin communicating with stakeholders to ensure clarity and prevent any misunderstandings.

Thank you for taking the initiative to send the email. I would appreciate it if all team members could be involved in future communications, as we are all part of the same team.

Additionally, I would like to discuss the various communication methods we can utilize, including email, phone calls, text messages, and any other options you might suggest. Please feel free to share any ideas you have.

Thank you once again for your collaborative spirit.

From: Tytiauna Goode <tgoode1@lamar.edu>
Sent: Thursday, February 13, 2025 9:31 AM
To: katia soto <katiaysoto@gmail.com>; Nilka Quinones <nilkaquinones2@gmail.com>
Cc: Karimi . Najera Garcia <knajera@lamar.edu>; originalines@hotmail.com <originalines@hotmail.com>
Subject: Re: Ransomeware Recovery Plan

Good Morning Team Leaders!

I am happy to see everyone working so diligently to formulate a plan to halt the ransomware attack. It seems that we all share many of the same viewpoints as it relates to resolving the issue. I want to reiterate my stance that it is important to include affected departments when making decisions about our plan of action. I'd like to loop the Financial Aid, IT, and Teaching and Learning departments as soon as we can to weigh in their input.

Additionally, I mentioned how important it is to me that we communicate with stakeholders as soon as possible. I understand some of you would like to wait until we have a more concise and agreed upon plan, but I think it is important to start communicating as we have known of this issue for a few days now. Below is the email I sent to students and parents:

> *Dear Students and Parents of Riverside Community College,*
>
> *I hope this message finds you well. I wanted to reach out to acknowledge the current situation regarding the ransomware attack and reassure you that we are actively working on a plan to resolve the issue as swiftly and securely as possible. We understand the anxiety this situation may cause, and we are committed to keeping you informed throughout the process.*
>
> *While the plan is still being finalized, please know that we will provide regular updates and keep you in the loop every step of the way. Your understanding and patience are greatly appreciated as we work diligently to address the challenges at hand. Our priority remains ensuring the security of your personal information and restoring full access to all affected systems as quickly as we can.*
>
> *Thank you for your cooperation, and I will continue to communicate with you as often as possible to ensure transparency during this process.*

I'd love to hear your thoughts on how we can continue making progress. I believe it would be a great idea to begin assembling our crisis response teams as soon as possible, so we can break down each area of concern into manageable steps. By incorporating staff input, we can ensure we approach this issue strategically and effectively.

Tytiauna Goode

Team Leader

From: katia soto <katiaysoto@gmail.com>
Sent: Wednesday, February 12, 2025 10:56 PM
To: Nilka Quinones <nilkaquinones2@gmail.com>
Cc: Karimi . Najera Garcia <knajera@lamar.edu>; Tytiauna Goode <tgoode1@lamar.edu>; originalines@hotmail.com <originalines@hotmail.com>
Subject: Re: Ransomeware Recovery Plan

Dear Team Leaders,

Thank you for your proactive approaches in addressing the recent cybersecurity incident and for fostering a collaborative environment to strengthen our institution's security. Given the ransomware attack that has affected Riverside Community College, we must ensure that our response is immediate, practical, resilient, and oriented toward long-term prevention.

1. Data Protection and Operational Continuity

To mitigate further risks and restore normal operations as soon as possible, we will take the following actions:

- System Containment and Security**:** The IT security team will isolate the compromised systems, assess vulnerabilities, and ensure no further data breaches occur.
- Strengthening Access Controls: Multi-factor authentication will be implemented, mandatory password changes will be enforced, and access to sensitive databases will be restricted.
- Alternative Access to Educational Materials: Temporary storage platforms will enable faculty members to continue their classes.
- Financial Aid Contingency Plan: We will work with institutions to ensure students receive financial support without significant delays.

2. Strengthening Communication and Trust with Stakeholders

A key principle is ensuring transparency and building trust. Our communication strategy will address all affected groups:

- With the IT Team and Administration:
  - A crisis response team will be established with regular meetings to coordinate actions and prevent fragmented information.
  - A structured communication channel will bridge the gap between the IT team and administrative staff.
  - Lessons Learned: At the end of the crisis management process, we will conduct a retrospective evaluation to improve future responses.
- With Students and Parents:
  - Regular updates will be sent via email and the student portal with information on implemented security measures.

  - A Frequently Asked Questions (FAQ) section will be available on the website to clarify concerns regarding data protection.
  - A live virtual forum will be organized where students and their families can directly express their concerns to the security and administrative teams.
- With Faculty and Administrative Staff:
  - Alternative solutions will be provided to access teaching materials.
  - Faculty members will be informed about the necessary procedures to regain access and receive technical assistance.
- With the Board of Trustees:
  - A detailed executive report will be presented, avoiding unnecessary technical details while providing key information on incident management and future measures.
  - External cybersecurity auditors will be engaged to assess risks and controls independently.

3. Establishing a Long-Term Security Culture

Beyond responding to this attack, we must adapt and evolve our cybersecurity strategies to prevent future incidents. To achieve this, we propose:

- Mandatory Cybersecurity Training:
  - Implement a tiered training program for students, faculty, and administrative staff.
  - Phishing attack simulations to strengthen awareness of digital threats.
- Enhancing System Security:
  - Regular security audits to identify and address vulnerabilities before they can be exploited.
  - Implementation of automated threat detection systems for rapid incident response.
- Data Governance and Access Policies:
  - Restriction of access to student information to only authorized personnel.
  - Application of access controls to ensure that only individuals with specific permissions can access critical information.
- Creation of a Cybersecurity Committee:
  - A multidisciplinary team consisting of IT professionals, faculty, and administrative staff will be established to oversee security measures and implement new policies.

4. A Collaborative and Innovative Approach for the Future

This incident should be a learning opportunity. Let us use this situation to strengthen our digital security strategy and reinforce trust within our institution.

To successfully navigate this challenge, we must remain adaptable, proactive, and committed to strengthening our institution's security. We can transform this incident into an opportunity for long-term resilience and improvement by fostering continuous learning, collaboration, and innovation. I appreciate your dedication and look forward to implementing effective solutions together.

Thank you for your leadership and commitment to digital security.

Sincerely,
Katia Y. Soto Hernandez,

Team Leader

On Wed, Feb 12, 2025 at 9:07 PM Nilka Quinones <nilkaquinones2@gmail.com> wrote:

Dear Team Leaders,
Thank you for bringing this matter to our attention. The recent cyber-attack has highlighted the vulnerabilities in our systems, disrupting financial aid processing, student information security, and access to essential academic resources. We must take a decisive and strategic approach to mitigate the current impact and prevent future incidents.

I fully support the notion that a multifaceted, proactive approach is essential. While no single solution can eliminate the risk of cyber threats, we have an opportunity to implement innovative strategies that will strengthen our cybersecurity posture and foster a security-conscious culture across our institution.

Strategic Priorities & Recommended Actions

1. Strengthening Communication & Stakeholder Engagement

The technical response often takes priority during cybersecurity incidents, but effective communication is equally critical. Misformation and uncertainty can erode trust among students, faculty, and stakeholders without clear and timely updates. I propose a structured, multi-tiered communication strategy to ensure transparency and alignment:

- Admin & IT Collaboration:
    - Form a dedicated cybersecurity response task force consisting of IT security experts, administrative leaders, and key decision-makers.
    - Implement real-time coordination mechanisms between IT teams and administration to ensure a unified and rapid response to threats.
    - Develop a post-incident review process to analyze response effectiveness and make necessary improvements.
- Communication with Students & Parents:
    - Provide regular status updates on system restoration efforts and clearly outline what steps students need to take regarding financial aid, class schedules, and account security.
    - Offer a dedicated cybersecurity helpdesk to assist students and parents with any concerns related to personal data protection.
    - Implement cyber hygiene awareness campaigns to educate students and parents on best practices for safeguarding their personal information.
- Board Members & Team Leaders:
    - Hold specialized briefing sessions with leadership teams to ensure institutional policies align with best cybersecurity practices.

  - Advocate for long-term investments in cybersecurity infrastructure and staff training to prevent future breaches.

2. Ensuring Continuity in Teaching & Learning

One of the most immediate consequences of a cyber-attack is the inability to access essential teaching materials, disrupting faculty workflow and student learning. We must establish redundant systems and alternative access solutions to ensure academic continuity:

- Develop a Secure Cloud-Based Backup System:
  - Ensure that all course materials, assignments, and grading data are regularly backed up to secure cloud storage that remains accessible even during cyber incidents.
  - Faculty and staff training on proper data backup procedures is required to reduce reliance on vulnerable local storage systems.

- Implement Temporary Alternative Access Methods:
  - In a significant disruption, provide faculty with offline access options for critical materials.
  - Establish emergency IT support teams to assist faculty and students in restoring access to learning materials.

- Strengthen Faculty Preparedness & Digital Literacy:
  - Conduct mandatory cybersecurity training for educators to ensure they can identify potential security threats and respond effectively to system disruptions.
  - Guide best practices for securing personal and professional accounts to prevent phishing attacks and unauthorized data access.

3. Enhancing Data Security & Preventative Measures

While addressing the immediate crisis is necessary, it is equally important to implement proactive measures that reduce the likelihood of future cyber-attacks. A robust cybersecurity framework should include the following:

- Strict Access Control Policies:
  - Implement role-based access controls (RBAC) to ensure that sensitive student data is only accessible to authorized personnel.
  - Multi-factor authentication (MFA) is required across all institutional systems to prevent unauthorized logins.

- Continuous Network Monitoring & Threat Detection:
  - Deploy AI-powered security tools to detect and respond to potential threats in real time.
  - Schedule regular penetration testing and vulnerability assessments to identify weaknesses before attackers do.

- Cybersecurity Training & Culture Development:
  - Establish a mandatory cybersecurity education program for faculty, staff, and students.
  - Conduct simulated phishing attack drills to teach employees to recognize and report suspicious activity.

- Strengthen Vendor & Third-Party Security Compliance:
    - Conduct cybersecurity audits on all third-party vendors who handle sensitive institutional data.
    - Require vendors to meet stringent security standards, including encryption and authentication protocols.

4. Establishing a Forward-Thinking Cybersecurity Culture

Beyond technical solutions, we must embed cybersecurity awareness into our institutional culture. Cyber threats evolve rapidly, and maintaining security requires continuous adaptation and education.

- Encourage a Culture of Accountability:
    - Make cybersecurity a shared responsibility across all departments rather than an isolated IT function.
    - Recognize and reward staff members who contribute to strengthening cybersecurity awareness and best practices.

- Develop a Long-Term Cybersecurity Roadmap:
    - Establish a dedicated cybersecurity committee to evaluate policies regularly, recommend improvements, and stay ahead of emerging threats.
    - Secure ongoing budget allocations for cybersecurity infrastructure and staff training initiatives.

A **Call for Innovation & Collaboration**

Each of you brings valuable expertise to this discussion, and we have a unique opportunity to reshape our cybersecurity framework with innovation and foresight. While established protocols provide a foundation, we must not be bound by past practices alone. This is our moment to implement forward-thinking, resilient security measures to safeguard our institution long-term.

To ensure a quick and strategic resolution, I request an immediate response from all leaders outlining the critical actions we must take in the short and long term. Your contributions will allow us to assess current vulnerabilities, implement urgent measures, and establish a sustainable security framework that protects our institution in the future.

Please share your insights and recommendations to help shape a well-informed, action-oriented strategy. Your expertise is invaluable, and through our collective leadership, we can transform this challenge into an opportunity to build lasting resilience and drive meaningful innovation.

We will resolve the crisis and build a foundation for sustained security, trust, and operational excellence. Thank you for your commitment to this critical initiative. I look forward to our collective leadership in securing our institution’s future.

Best regards,

Nilka V Quinones Rodriguez

Team Leader

From: Karimi . Najera Garcia <knajera@lamar.edu>
Date: Tuesday, February 11, 2025 at 10:34 AM
To: Tytiauna Goode <tgoode1@lamar.edu>,
nilkaquinones2@gmail.com <nilkaquinones2@gmail.com>,
katiaysoto@gmail.com <katiaysoto@gmail.com>,
originalines@hotmail.com <originalines@hotmail.com>
Subject: Re: Ransomeware Recovery Plan

Tytianna,

Thank you for providing such a comprehensive report; your efforts in ensuring we address the critical aspects of the plan are commendable.

I would be more than happy to address some of your concerns. However, I would also appreciate input from the other leaders to develop a plan that is both innovative and effective.

1. I believe this is an excellent idea. It will enhance our communication with stakeholders and allow us to address issues as they arise. Additionally, being open and transparent will help alleviate stakeholder concerns.

2. Yes, I think it is essential to have someone serve as the liaison. It is extremely important that everyone who has been impacted is included in this process. Is there a way to generate a report? I would like us to proactively consider how we can compile this report at the earliest opportunity.

3. I believe this approach will be beneficial in providing support. We will need to collaborate with our counselors to assist with this component. What is your perspective on this?

4. This is a commendable idea; we need to develop a plan that eases the process for all stakeholders. My goal is to avoid placing additional stress on anyone involved.

I would appreciate hearing from the other leaders regarding this matter.

From: Tytiauna Goode <tgoode1@lamar.edu>
Sent: Monday, February 10, 2025 2:20 PM
To: Karimi . Najera Garcia <knajera@lamar.edu>;
nilkaquinones2@gmail.com <nilkaquinones2@gmail.com>;
katiaysoto@gmail.com <katiaysoto@gmail.com>;
originalines@hotmail.com <originalines@hotmail.com>
Subject: Re: Ransomeware Recovery Plan

Hello Karimi and Team,

First of all, thank you for your thoughtful email, Karimi. I truly appreciate the clear steps you've outlined in addressing the ransomware attack. Your emphasis on proactive measures like security training, transparency, and creating a culture of cybersecurity aligns with the need for long-term improvement, which I completely agree with.

As a leader who values collaboration and shared decision-making, I want to engage with your ideas and add my perspective on how we can approach this crisis together. We're all in this together, and while each of us brings our unique strengths to the table, I believe our combined efforts will make us stronger.

Major Concern: One key recommendation I'd like to add to our plan is a clear strategy for immediate communication and transparency. As soon as possible, I suggest sending an email to faculty, staff, students, and parents explaining the situation in simple, non-technical terms, outlining the immediate actions we're taking. Additionally, I propose creating an interactive webpage where stakeholders can submit their concerns, which will be addressed through live responses or regular updates to ensure everyone stays informed and engaged throughout the process.

As a collaborative leader, I believe this effort should involve a diverse group. IT will manage the technical aspects, while faculty and student leaders can ensure we address specific community concerns. The communications team will help craft clear, consistent updates. By working together, we can create a communication plan that's both informative and responsive.

In addition to the communication strategies outlined, I would recommend forming a crisis response team that includes not just technical staff, but also faculty, financial aid representatives, and student leaders. This diverse team will help us address both the technical and human aspects of the crisis. Regular meetings and an active feedback loop from all departments will be crucial in keeping everyone aligned as the situation evolves. Furthermore, I propose establishing open office hours for students and faculty to directly discuss concerns, providing emotional support during this difficult time. Lastly, I envision a continuous feedback process through town hall meetings or feedback forms to ensure our response remains in tune with the needs of the campus community.

Additionally, I do have some questions and thoughts about your current plan that I'd like to discuss with the team:

1. Stakeholder Engagement & Communication

- I agree that communication is critical, and I appreciate your focus on providing timely updates. I am wondering if there might be a more collaborative way we can involve our stakeholders (specifically faculty and students) throughout the process.

- **Question: Could we set up a regular forum or feedback mechanism where key stakeholders can provide input as the situation unfolds? This would help us make sure we are responding in real-time to the challenges they're facing and keep them involved in the process. I'd love to hear your thoughts on this.**

2. Crisis Response Team

- I really like your idea of creating a crisis response team. You've mentioned bringing in experts from IT, financial aid, and teaching and learning, which is fantastic. However, I think it's crucial to make sure we are not only addressing the technical aspects of the issue but also the emotional and logistical needs of the community.
- **Question: How can we ensure that the voices of faculty, students, and staff, who are directly impacted by this situation, are fully incorporated into the decision-making process? For example, might we want to include faculty representatives in a more formal decision-making role to help guide the creation of alternative teaching plans or access to materials?**

3. Empathy & Emotional Support

- You've highlighted the importance of transparency and reassurance, which I fully support. However, given the emotional toll a crisis like this can take, I believe we should place even more emphasis on providing emotional support to our stakeholders.
- **Suggestion: In addition to a hotline for financial aid concerns, what if we also set up a support group or virtual office hours for faculty and students to express their concerns and receive real-time guidance on how we can support them? This could help us build trust and ease anxiety as we work through the crisis.**

4. Long-Term Security Measures & Adaptability

- I completely agree that long-term cybersecurity measures are essential. After the immediate crisis is resolved, I think it's equally important to keep the conversation going within our community.
- **Question: How can we include faculty, staff, and students in the post-crisis evaluation of what worked and what didn't? This would help us create a sustainable cybersecurity culture together, where everyone feels empowered to contribute to building resilience.**
- **Suggestion: Maybe we can include the IT department in the creation of an ongoing forum to continuously collect data. They are the experts in the field, and should know what data we need to collect.**

I am looking forward to hearing your thoughts,

From: Karimi . Najera Garcia <knajera@lamar.edu>
Sent: Monday, February 10, 2025 12:56 PM
To: nilkaquinones2@gmail.com <nilkaquinones2@gmail.com>; katiaysoto@gmail.com <katiaysoto@gmail.com>; originalines@hotmail.com <originalines@hotmail.com>; Tytiauna Goode <tgoode1@lamar.edu>
Subject: Ransomeware Recovery Plan

Good morning, Team Leaders,

I would like to bring to your attention a recent cyber attack and the subsequent issue with financial aid processing within our school. To address this matter collaboratively, I have outlined a few suggestions for potential solutions. There are several proactive measures that we can implement to mitigate the risk of data breaches. It is important to recognize that no singular solution can completely eliminate the possibility of such incidents; rather, a multifaceted approach is essential. Ongoing assessment and enhancement of cybersecurity protocols, coupled with current training for both students and educators, are crucial components of an effective strategy.

I welcome your input and would appreciate hearing your thoughts and ideas as we work through this challenge together. Your contributions are essential to our team's success.

I look forward to reviewing everyone's ideas and proposals.

Establishing a Cybersecurity-Focused Culture

- It is essential to cultivate a comprehensive understanding among the school community regarding the importance of digital security. This includes providing training that outlines the typical methods employed by cybercriminals to infiltrate and exploit school networks. By doing so, we can effectively address any knowledge deficits and enhance the overall training process.

Limit access to data.

- Implementing access restrictions to sensitive data is essential. Passwords play a critical role in this process; therefore, the school and district leaders must train staff on the significance of developing robust passwords and utilizing multi-factor authentication as part of the data security policy.

I would appreciate it if you could provide me with at least 2-3 additional recommendations for securing sensitive data.

During an incident, schools frequently emphasize their technical response, sometimes overlooking the importance of communication. However, effective communication with staff, stakeholders, customers, and the media is essential for influencing the school's overall perception.

Communication with admin and IT

- The initial step is to assemble the response team to the extent possible, evaluate the circumstances, and execute the predetermined response plans. It is essential to assess the current facts of the situation, including the nature and scope of the incident, the individuals and systems impacted, potential changes in the situation, and the schedule for providing updates.

- Sharing valuable insights and lessons learned from the incident response process, along with the actions implemented to enhance resilience and preparedness for future incidents. **(area of growth)**
- Following the incident, it is important to evaluate our communication response and adjust our strategy accordingly to incorporate any necessary improvements.

This process may involve engaging with both internal and external stakeholders to gather feedback on how the message was received and identify areas for enhancement. **(New ideas and strategies are welcomed)**

- We must communicate consistently with engineers, the admin team, and IT personnel. Their expertise will assist us in distinguishing established facts from emerging theories, enabling us to relay only the information we are confident in.

Communication with students and parents:

- Ensuring open lines of communication with both parents and students by providing timely updates and responding to inquiries in a transparent manner to effectively address negative publicity and misinformation.
- Outline Immediate Actions: We need to inform them of the measures we are implementing to address the situation, such as changing passwords, contacting the appropriate services, and conducting a malware scan.

- We need to assure them that we are actively addressing the issue and are implementing measures to safeguard their information.

Unable to access teaching materials:

- We need to stay composed and informative. Maintain a positive and reassuring tone to minimize unnecessary anxiety for those unable to access teaching materials.

- We need to adapt to the situation. Help customize the teaching materials and focus according to the evolving circumstances of the cyberattack.

Communicating with board members:

It is crucial that presentations address key questions regarding how cybersecurity initiatives align with the school's core mission and objectives. Most importantly, we need to avoid overly technical explanations, ensuring that each point is presented at a high level to promote understanding while providing sufficient detail for the board to gain a clear overview.

Input from Others

- Boards should engage with various groups, including internal auditors, to gain insights into cyber risks. Additionally, external auditors can offer valuable perspectives on cybersecurity controls related to financial reporting processes.

- Engage with the board to discuss the importance of incorporating external perspectives, such as third-party assessments on key risk areas and practices tailored to our school's size. Request that the findings be communicated directly to the board.

Team leaders, I believe that proactively developing new strategies for protecting sensitive data can benefit not only our students and staff members but also ourselves. Let us view this incident as a valuable lesson and move forward with an innovative plan for the future.

I recognize that each of you has a wealth of knowledge to contribute. While I understand there are established protocols for situations like this, let us embrace the opportunity for change and strive to create something more innovative.

> > > > **I am reaching out to you because each of you possesses unique skills and expertise that can significantly enhance our efforts.**
> > > >
> > > > Thank you,
> > > >
> > > > Team Leader
> > > > Karimi Najera-Garcia
> > > >
> > > > CONFIDENTIALITY: Any information contained in this e-mail (including attachments) is the property of The State of Texas and unauthorized disclosure or use is prohibited. Sending, receiving or forwarding of confidential, proprietary and privileged information is prohibited under Lamar Policy. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.
> > >
> > > CONFIDENTIALITY: Any information contained in this e-mail (including attachments) is the property of The State of Texas and unauthorized disclosure or use is prohibited. Sending, receiving or forwarding of confidential, proprietary and privileged information is prohibited under Lamar Policy. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.
> > > CONFIDENTIALITY: Any information contained in this e-mail (including attachments) is the property of The State of Texas and unauthorized disclosure or use is prohibited. Sending, receiving or forwarding of confidential, proprietary and privileged information is prohibited under Lamar Policy. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.
> >
> > CONFIDENTIALITY: Any information contained in this e-mail (including attachments) is the property of The State of Texas and unauthorized disclosure or use is prohibited. Sending, receiving or forwarding of confidential, proprietary and privileged information is prohibited under Lamar Policy. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

CONFIDENTIALITY: Any information contained in this e-mail (including attachments) is the property of The State of Texas and unauthorized disclosure or use is prohibited. Sending, receiving or forwarding of confidential, proprietary and privileged information is prohibited under Lamar Policy. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

CONFIDENTIALITY: Any information contained in this e-mail (including attachments) is the property of The State of Texas and unauthorized disclosure or use is prohibited. Sending, receiving or forwarding of confidential, proprietary and privileged information is prohibited under Lamar Policy. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

Leadership Simulation Assignment

Karimi Garcia	Transformational Leader
Tytiauna Goode	Collaborative Leader
Maria Fernandez	Servant Leader
Nilka Quinones	Strategic Leader
Katia Soto	Adaptive Leader

References

Barron, B., & Henderson, M. (1995). Strategic leadership: A theoretical and operational definition. *Journal of Instructional Psychology,* 22(2), 178. https://research-ebsco-com.libproxy.lamar.edu/c/2rtsa2/viewer/html/oxgpdf66xb

Daloisio, T. (n.d.). *Servant leadership in education: Putting people first for greater impact.* Washington Leadership Partners. https://washingtonleadershippartners.com/blog/servant-leadership-in-education-putting-people-first-for-greater-impact?form=MG0AV3

Davenport, G. (2022). Adaptive leadership for school equity. *Educational Leadership*, *79*(6), 22–25.https://research-ebsco-com.libproxy.lamar.edu/linkprocessor/plink?id=bcc68898-7136-34ba-bdb3-31aac45aa993

Davies, B. (2003). Rethinking Strategy and Strategic Leadership in Schools. *Educational Management Administration & Leadership,* 31(3). https://www.researchgate.net/publication/275455097_Rethinking_Strategy_and_Strategic_Leadership_in_Schools

DeWitt, P. (2016). Collaborative leadership: Six influences that matter most. *Vanguard,* 5-8. https://saanys.org/wp-content/uploads/2019/03/Vanguard-FALL2016-collaborative-leadership.pdf

Gartner. (2019, November 5). *The 15-minute, 7-slide security presentation for your board of directors*. https://www.gartner.com/smarterwithgartner/the-15-minute-7-slide-security-presentation-for-your-board-of-directors

Gutierrez, N. (2024, April 8). Strategies to prevent school data breaches effectively. https://preyproject.com/blog/data-breaches-in-schools-what-measures-you-should-take

Heifetz, R., Grashow, A., & Linsky, M. (2009). *The practice of adaptive leadership: Tools and tactics for changing your organization and the world*. Harvard Business Press.

Hinton, L. Gaisie, N., Schake, K., & Zoubak, E.(2024). Linking principal adaptive leadership to teacher performance: The mediating effect of collaborative school culture. *Journal of Social Studies Education Research*, *15*(4), 17–41. https://research-ebsco-com.libproxy.lamar.edu/linkprocessor/plink?id=d45eb008-1bdb-3dc5-a3de-ba940b87602f

Joseph, M. (2018, January 30). *How to be a collaborative leader.* eSchool News. https://www.eschoolnews.com/educational-leadership/2018/01/30/collaborative-leader/

Keiser University. (2023, December 30). *Servant leadership in education: Why it's needed and what it can accomplish. Keiser University.* https://www.keiseruniversity.edu/servant-leadership-in-education-why-its-needed-and-what-it-can-accomplish/

Khamisa, A. (2023, October 24). *Profiles in servant leadership: 12 famous leaders.* Azim Khamisa. https://azimkhamisa.com/servant-leader-profiles/

Leadershipahoy! (2020, October 26). *Servant leadership! How to become a good servant leader? Is servant leadership the right choice?* [Video]. Youtube. Tube.https://www.youtube.com/watch?v=f1WWXyXFOkU

Sandling, J. (2024). *10 Principles of servant leadership.* Team Gantt. https://www.teamgantt.com/blog/servant-leadership

Shoemaker, P. J., Krupp, S., & Howland, S. (2013). *Strategic leadership: The essential skills*. Harvard Business Review. https://hbr.org/2013/01/strategic-leadership-the-esssential-skills

Theophille, L. [TEDxSaclay]. (2020, January 23). *Servant leadership: how to lead with the heart?* [Video]. Youtube. https://www.youtube.com/watch?v=vZ0gave2WJc

Ugochukwu, C. (2024, January 29). *Transformational leadership theory: Inspire & motivate.* Simply Psychology. https://www.simplypsychology.org/what-is-transformational-leadership.html

University of Massachusetts Global. (2021). What is transformational leadership and why is it effective?: UMass Global. www.umassglobal.edu. https://www.umassglobal.edu/news-and-events/blog/what-is-transformational-leadership#:~:text=A%20transformational%20leadership%20style%20inspires,leaders%20reach%20their%20full%20potential

Williams, H. S., & Johnson, T. L. (2013). Strategic Leadership in Schools. *Project Innovation Austin LLC, 133(3)*. https://go-gale-com.libproxy.lamar.edu/